Web Application Vulnerability Reconnaissance Report on

www.bjnetworksolution.xyz (66.29.153.49)

Prepared By: Bolaji Bakare

Date: Nov 3, 2025

1. Executive Summary

This report provides an assessment of potential vulnerabilities discovered during the reconnaissance phase for the target domain www.bjnetworksolution.xyz. The analysis focuses on domain enumeration, network mapping, and identification of misconfigurations or exposed services that could be exploited by malicious actors.

A comprehensive vulnerability assessment was performed using Tenable Nessus Essentials to identify potential security weaknesses, misconfigurations, and exposure points within the web application.

The scan was completed successfully and identified four informational findings, with no vulnerabilities detected at critical, high, medium, or low severity levels.

Although the application does not present an immediate or elevated risk, certain configuration-related observations warrant attention. If left unaddressed or if combined with other attack vectors, these findings could potentially degrade the overall security posture.

To further harden the environment, recommendations include optimizing server configuration settings and refining HTTP request handling practices in alignment with security best practices.

Scope of Assessment

- **Target Host: bjnetworksolution.xyz**
- **Scan Type: Web Application Tests**
- **Scanner: Nessus Essentials (Local Scanner)**
- **Scan Duration: 27 minutes**
- **Ports Identified: 80/tcp, 587/tcp**

Summary of Findings

Severity Breakdown:

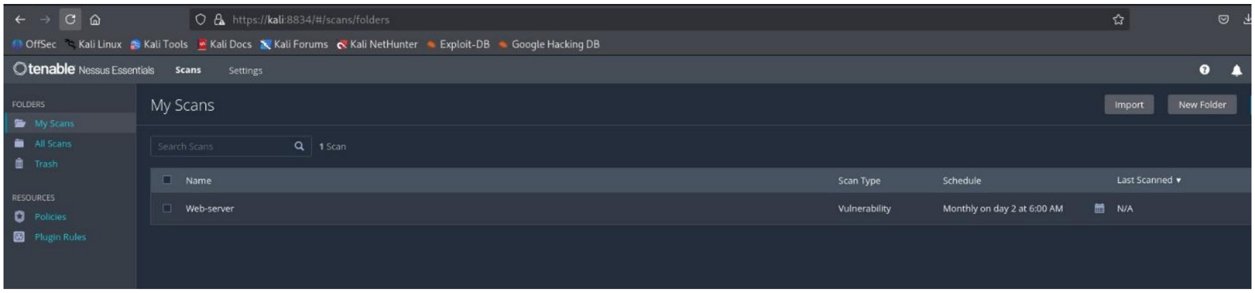
- **Critical: 0**
- **High: 0**
- **Medium: 0**
- **Low: 0**
- **Informational: 4**

Detailed Findings

Below are the detailed findings categorized by plugin and relevance.

Finding 1: Scan Dashboard Overview

Figure 1: Nessus Scan Summary Dashboard

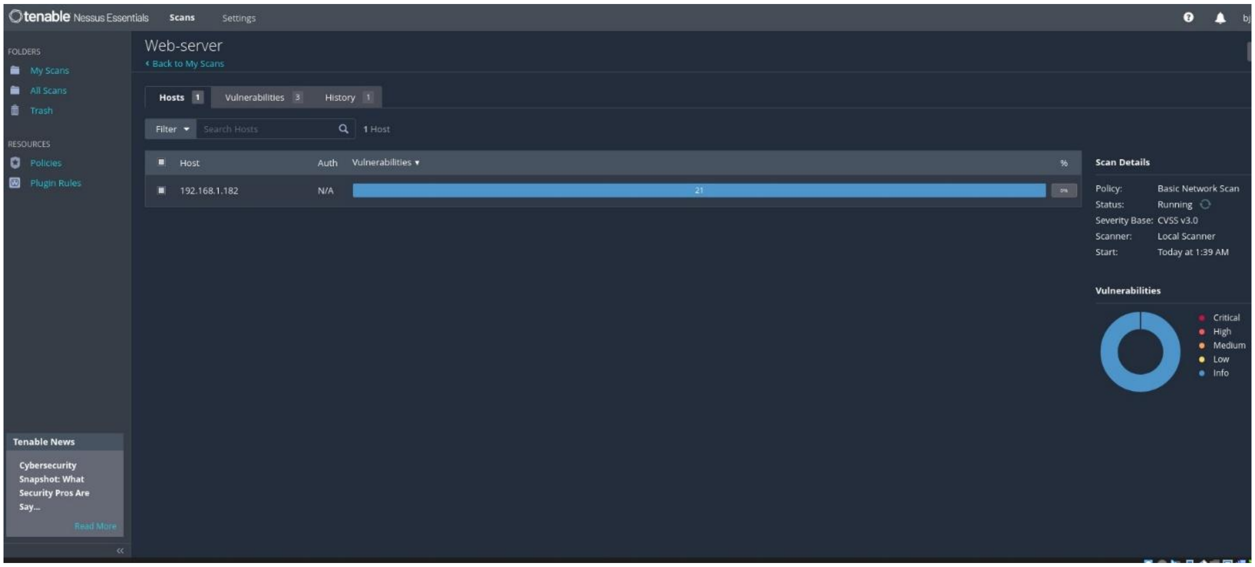


https://kali:8834/#/scans/folders

My Scans

1 Scan

☐	Name	Scan Type	Schedule	Last Scanned ▾
☐	Web-server	Vulnerability	Monthly on day 2 at 6:00 AM	N/A



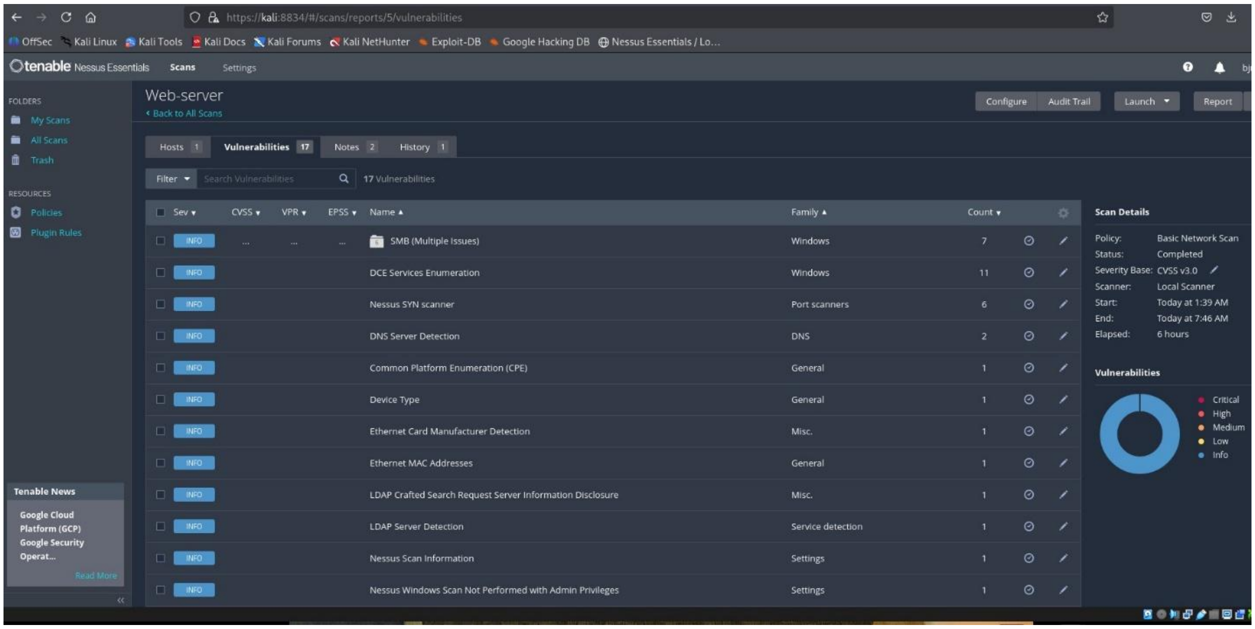
Web-server

Host	Auth	Vulnerabilities	%
192.168.1.182	N/A	21	0%

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:39 AM

Vulnerabilities



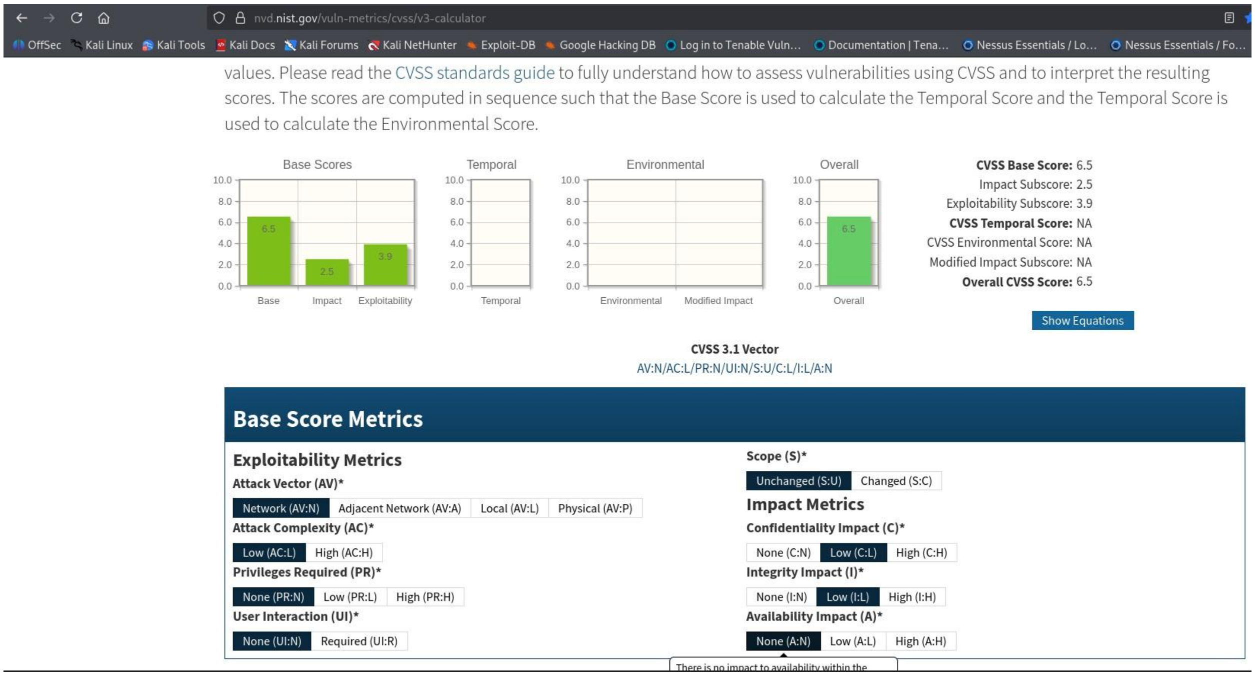
Web-server

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO	...	...	...	SMB (Multiple Issues)	Windows	7
INFO				DCE Services Enumeration	Windows	11
INFO				Nessus SYN scanner	Port scanners	6
INFO				DNS Server Detection	DNS	2
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				LDAP Crafted Search Request Server Information Disclosure	Misc.	1
INFO				LDAP Server Detection	Service detection	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus Windows Scan Not Performed with Admin Privileges	Settings	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:39 AM
End: Today at 7:46 AM
Elapsed: 6 hours

Vulnerabilities



values. Please read the CVSS standards guide to fully understand how to assess vulnerabilities using CVSS and to interpret the resulting scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 6.5
Impact Subscore: 2.5
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 6.5

CVSS 3.1 Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*
[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*
[✓ None (PR:N)] Low (PR:L) High (PR:H)

User Interaction (UI)*
[✓ None (UI:N)] Required (UI:R)

Scope (S)*
[✓ Unchanged (S:U)] Changed (S:C)

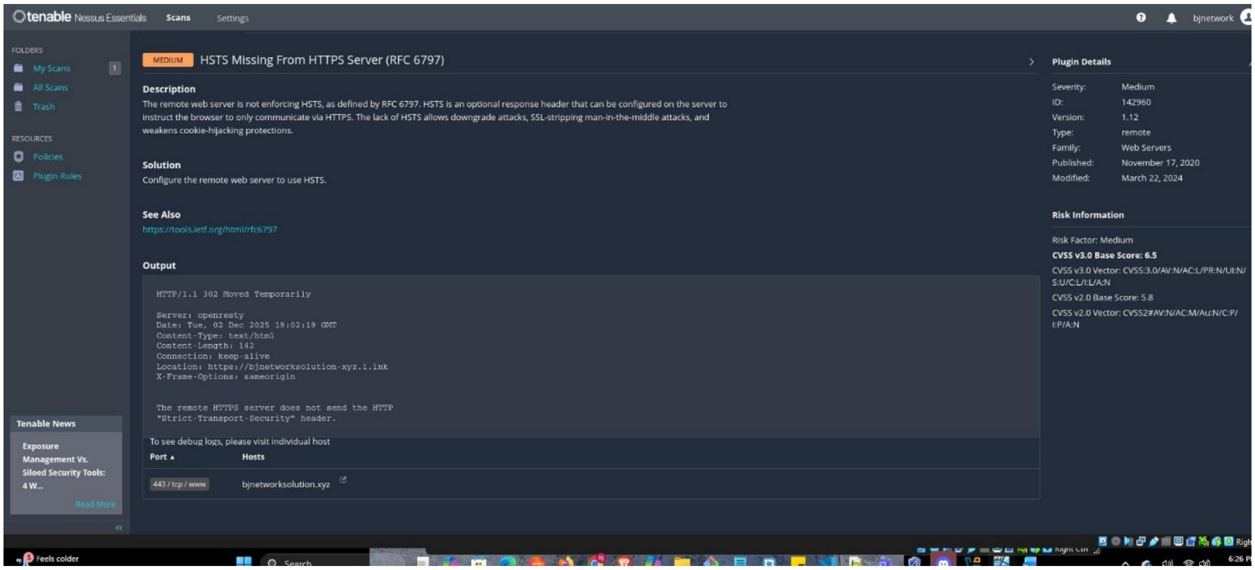
Impact Metrics

Confidentiality Impact (C)*
None (C:N) [✓ Low (C:L)] High (C:H)

Integrity Impact (I)*
None (I:N) [✓ Low (I:L)] High (I:H)

Availability Impact (A)*
[✓ None (A:N)] Low (A:L) High (A:H)

There is no impact to availability within the



MEDIUM HSTS Missing From HTTPS Server (RFC 6797)

Description
The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Solution
Configure the remote web server to use HSTS.

See Also
https://tools.ietf.org/html/rfc6797

Output

```
HTTP/1.1 302 Moved Temporarily

Server: openresty
Date: Tue, 02 Dec 2025 19:02:19 GMT
Content-Type: text/html
Content-Length: 142
Connection: keep-alive
Location: https://bjnetworksolution-xyz.1.ink
X-Frame-Options: sameorigin


The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

To see debug logs, please visit individual host

Port ▲	Hosts
443 / tcp / www	bjnetworksolution.xyz

Plugin Details

Severity:	Medium
ID:	142960
Version:	1.12
Type:	remote
Family:	Web Servers
Published:	November 17, 2020
Modified:	March 22, 2024

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v2.0 Base Score: 5.8
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

Recommendations

- **Restrict HTTP methods to GET, POST, and HEAD only.**
- **Ensure proper 404 response handling for non-existent files.**
- **Harden and monitor port 587 (Mail Submission Port).**
- **Implement firewall restrictions for unused ports.**
- **Regular vulnerability scanning and penetration testing.**

Conclusion

The Nessus web application scan for bjnetworksolution.xyz shows a relatively secure environment WITH NO CRITICAL OR EXPLOITABLE VULNERABILITIES detected. However, configuration weaknesses related to HTTP methods, port exposure, and request handling should be addressed to ensure stronger security and reduce the attack surface.

By implementing the recommended hardening steps, the organization can enhance the robustness of its web infrastructure and better protect against future threats.